

# MOBILE COMMUNICATION NETWORK, TERMINAL, PACKET COMMUNICATION CONTROL METHOD, AND GATEWAY UNIT

**Patent number:** JP2001326697

**Publication date:** 2001-11-22

**Inventor:** TAKEDA SACHIKO; INAI HIDENORI; OISHI TAKUMI;  
SHIBATA JIRO

**Applicant:** HITACHI LTD

**Classification:**

- International: H04L12/66; H04L12/28; H04L12/56; H04L29/02

- european:

**Application number:** JP20000149808 20000517

**Priority number(s):**

**Also published as:**



EP1156626 (A2)

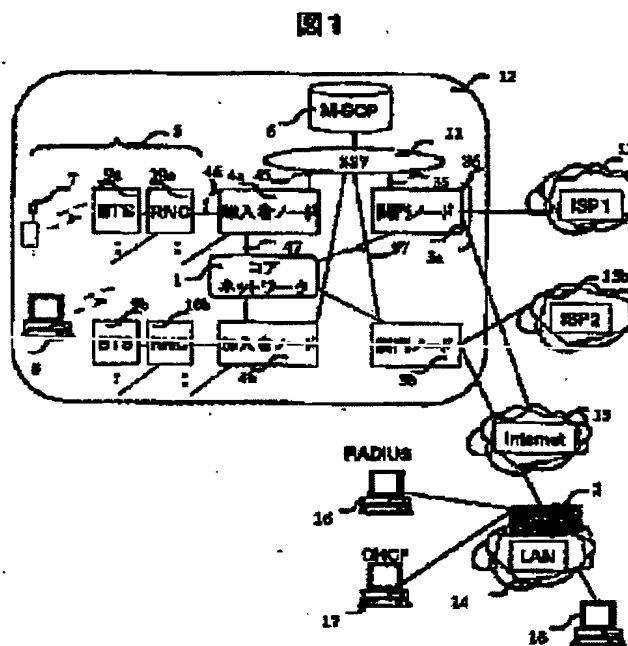
US2001048686 (A)

JP2001326697 (A)

## Abstract of JP2001326697

**PROBLEM TO BE SOLVED:** To provide a mobile VPN service without having to use a mobile tunnel in an IPv6 mobile packet communication network.

**SOLUTION:** A mobile terminal transmits a control signal to enable packet transmission reception to a gateway node 3. The gateway node 3 discriminates presence or absence of a mobile VPN service request from connection destination information included in the signal. The gateway node 3 detecting the mobile VPN service request informs the mobile terminal about an IP address of the gateway node 3 via a subscriber node 4. The mobile terminal sets an IPv6 header 210 and an IPv6 path control header 220, so that the gateway node 3 relays the transmission packet without fail.



Data supplied from the esp@cenet database - Patent Abstracts of Japan

BEST AVAILABLE COPY

(51) Int. Cl. <sup>7</sup>	識別記号	F I	テマコード (参考)
H04L 12/66		H04L 11/20	B 5K030
12/28		11/00	310 B 5K033
12/56		11/20	102 A 5K034
29/02		13/00	301 B

審査請求 未請求 請求項の数15 O L (全15頁)

(21) 出願番号 特願2000-149808 (P 2000-149808)

(22) 出願日 平成12年5月17日 (2000. 5. 17)

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 武田 幸子

東京都国分寺市東恋ヶ窪一丁目280番地

株式会社日立製作所中央研究所内

(72) 発明者 井内 秀則

東京都国分寺市東恋ヶ窪一丁目280番地

株式会社日立製作所中央研究所内

(74) 代理人 100075096

弁理士 作田 康夫

最終頁に続く

(54) 【発明の名称】 移動体通信網、端末装置、パケット通信制御方法、及び、関門装置

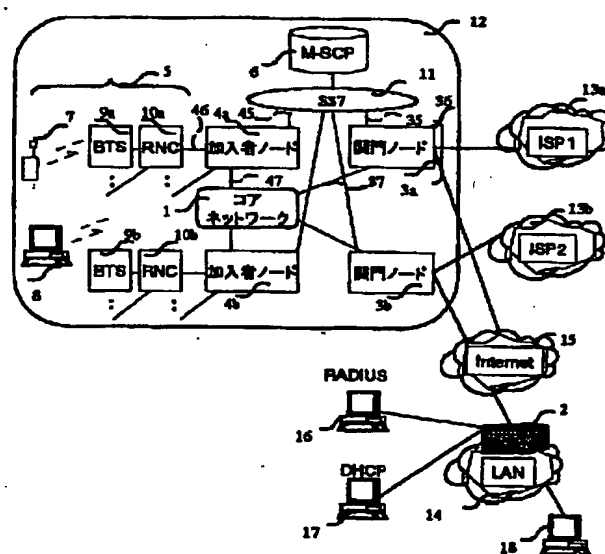
(57) 【要約】

【課題】 IPv6 移動体パケット通信網において、モバイルトンネルを利用することなくモバイルVPNサービスを提供する。

【解決手段】 移動端末は、関門ノード3にパケット送受信を可能にするための制御信号を送信する。関門ノード3は、上記信号に含まれる接続先情報から、モバイルVPNサービス要求の有無を判別する。モバイルVPNサービス要求を検出した関門ノード3は加入者ノード4経由で移動端末に上記関門ノード3のIPアドレスを通知する。移動端末は、送信パケットが必ず上記関門ノード3を中継するようにIPv6ヘッダ210とIPv6経路制御ヘッダ220を設定する。

【効果】 IPv6 機能を活用することより、移動体パケット通信網において、モバイルトンネルを利用することなくモバイルVPNサービスの提供が可能になる。

図1



BEST AVAILABLE COPY

## 【特許請求の範囲】

【請求項 1】 加入者装置と、該加入者装置との通信手段を有する複数の閥門装置とを有し、

上記加入者装置は、端末装置からの通信要求を受け取ると、上記通信要求に対応する閥門装置を選択し、上記選択された閥門装置は、上記通信要求に対応する通信網または通信網上の装置を特定するとともに、上記選択された閥門装置のアドレス情報を上記端末装置に通知することを特徴とする移動体通信網。

【請求項 2】 上記端末装置の加入者情報を記憶したサービス制御装置をさらに有し、

上記閥門装置は、上記加入者情報から上記通信要求に対応する通信網または通信网上的装置を特定する請求項 1 記載の移動体通信網。

【請求項 3】 上記選択された閥門装置は上記通信要求において特定サービスが指定されていない場合には、上記選択された閥門装置のアドレス情報を上記端末装置に通知しない請求項 1 記載の移動体通信網。

【請求項 4】 移動体通信網の加入者装置に APN を含む通信要求を行い、

上記 APN により特定される閥門装置から該閥門装置のアドレス情報を受取り、該アドレス情報を利用してパケットの IPv6 ヘッダ及び IPv6 経路制御ヘッダを組み立てて、該パケットを送信する端末装置。

【請求項 5】 接続先となる通信網または通信网上的装置を特定する情報を上記通信要求に含める請求項 4 に記載の端末装置。

【請求項 6】 上記移動体通信網に特定サービスを要求しない場合には、通常の IPv6 パケットを送信する請求項 4 記載の端末装置。

【請求項 7】 端末装置と、加入者装置と、加入者装置や他の通信網との通信手段を有する閥門装置とからなるパケット通信網において、

上記加入者装置と上記閥門装置は、加入者毎の位置情報やサービス情報を備えるサービス制御装置との通信手段を備え、

上記閥門装置は、他の通信網を介して企業網内の装置と通信する手段を備え、

上記端末装置は、上記パケット通信網上或いは他の通信网上的装置と情報の送受信を可能にするため、上記加入者装置経由で閥門装置に制御信号を送信し、

上記閥門装置は、加入者装置から送信された制御信号に含まれる接続先情報から、企業網内装置との通信要求を検出する第 1 の手段を備え、

上記閥門装置が企業網内装置との通信要求を検出した時、上記閥門装置のアドレス情報を含む制御信号を上記加入者装置に送信し、

上記加入者装置が、上記閥門装置のアドレス情報を含む制御信号を上記端末装置に送信する第 2 の手段を備え、

上記端末装置が、受信信号に上記閥門装置のアドレス情

報が含まれる時、上記閥門装置のアドレス情報を IPv6 ヘッダ情報作成時に適用し、上記端末装置が送信するパケットが、上記特定閥門装置を必ず中継するように、IPv6 パケットを組み立てる第 3 の手段を備えることにより、

上記端末装置が上記企業網内の装置宛に送信するパケットが、必ず上記特定閥門装置を経由することを特徴とするパケット通信制御方法。

【請求項 8】 上記端末装置が、上記加入者装置から閥門装置のアドレス情報を含む制御信号を受信した時、上記閥門装置のアドレス情報を利用して、IPv6 ヘッダと IPv6 経路制御ヘッダを作成し、

上記端末装置が送信するパケットが、上記特定閥門装置を必ず中継するように、パケットを組み立てる手段を備えることにより、

上記端末装置が上記企業網内の装置宛に送信するパケットが、必ず上記特定閥門装置を経由することを特徴とする請求項 7 に記載のパケット通信制御方法。

【請求項 9】 上記閥門装置が接続先の特定に利用する情報は、

上記加入者装置が上記サービス制御装置に記憶されている上記端末装置の加入者情報から上記端末装置の接続先情報を読み出して、閥門装置宛の制御信号に設定した接続先情報、或いは、端末装置がユーザによって上記端末装置に入力された接続先情報を加入者装置宛の制御信号に設定し、上記制御信号を受信した加入者装置が閥門装置宛の制御信号に設定した接続先情報であることを特徴とする請求項 7 に記載のパケット通信制御方法。

【請求項 10】 下線部分について明細書の記載がないと思われる端末装置と、加入者装置と、加入者装置や他の通信網との通信手段を有する閥門装置とからなるパケット通信網において、

上記加入者装置と上記閥門装置は、加入者毎の位置情報やサービス情報を備えるサービス制御装置との通信手段を備え、

上記閥門装置は、他の通信網を介して企業網内の装置と通信する手段を備え、

上記端末装置は、上記パケット通信網上或いは他の通信网上的装置と情報の送受信を可能にするため、上記加入者装置経由で上記閥門装置に制御信号を送信し、

上記閥門装置が上記加入者装置から受信した制御信号には、ユーザが設定した接続先情報、或いは、サービス制御装置から読み出された接続先情報が必ず含まれ、

上記閥門装置は、加入者装置から送信された制御信号に含まれる接続先情報から、企業網内装置との通信要求の有無を検出する第 1 の手段を備え、

第 1 の手段によって、上記閥門装置が企業網内装置との通信要求を検出した時、上記閥門装置が、上記閥門装置のアドレス情報を含む制御信号を上記加入者装置に送信し、

上記加入者装置が、上記閥門装置のアドレス情報を含む制御信号を上記端末装置に送信する第2の手段を備え、上記端末装置が受信した信号に上記閥門装置のアドレス情報が含まれる時、上記端末装置は上記閥門装置のアドレス情報を利用して、IPv6ヘッダとIPv6経路制御ヘッダを作成し、

上記端末装置が送信するパケットが、上記特定閥門装置を必ず中継するように、パケットを組み立てる第3の手段を備え、

第1の手段によって、上記閥門装置が企業網内装置との通信要求を検出しなかった時、上記閥門装置は上記閥門装置自身のアドレス情報を含まない制御信号を上記加入者装置に送信し、

上記加入者装置が、上記端末装置に上記閥門装置のアドレス情報を含まない制御信号を送信し、

上記端末装置は、受信信号に上記閥門装置のアドレス情報が含まれない時、通常のIPv6パケットを接続先に送信する手段を備え、

上記端末装置が、企業網内の装置宛にパケットを送信する場合には、上記端末装置が送信するパケットは、必ず上記特定閥門装置を経由し、

上記端末装置が、通常のIPv6パケットを接続先に送信する場合には、上記IPv6パケットは、各装置が保持する経路表に基づき、接続先に対して最適ルーティングされることを特徴とするパケット通信制御方法。

【請求項11】パケット通信網に接続されており、加入者装置や、他のパケット通信網上の装置や他網の装置との通信手段と、加入者毎の位置情報やサービス情報を備えるサービス制御装置との通信手段を備える閥門装置において、

他の通信網を介して企業網内の装置と通信する手段を備え、

加入者装置から移動端末のパケット送受信を可能にするための制御信号を受信し、上記制御信号に含まれる接続先情報から、企業網内の装置との通信が要求されていることを検出する第1手段を備えることを特徴とする閥門装置。

【請求項12】上記閥門装置が、上記第1の手段により、企業網内の装置との通信要求を検出すると、上記企業網内の装置と通信を行うため、上記閥門装置と企業網内と他の通信網とを接続する装置との間に上記移動端末用のコネクションを設定する機能を備えることを特徴とする請求項11に記載の閥門装置。

【請求項13】上記閥門装置が、上記第1の手段により、企業網内の装置との通信要求を検出すると、上記加入者装置に、上記閥門装置自身の識別情報を含む制御信号を送信することを特徴とする請求項11に記載の閥門装置。

【請求項14】パケット通信網に接続されており、端末装置や他の通信網との通信手段を有する閥門装置やパケ

ット通信網内の他の装置と通信を行う手段と、加入者毎の位置情報やサービス情報を備えるサービス制御装置と通信を行う手段を有する加入者装置において、上記閥門装置が他の通信網を介して企業網内の装置と通信する手段を有し、

上記端末装置が上記パケット通信網上或いは他の通信網上の装置と情報の送受信を開始する前に、上記閥門装置に、予め定められた手順に従ってパケットの送受信を可能にするための制御信号を送信すると、上記閥門装置は受信した制御信号から企業網内の装置との通信要求を検出し、

上記閥門装置から上記閥門装置自身の識別情報を含む制御信号を受信した場合に、上記端末装置宛に上記閥門装置の識別情報を含む制御信号を送信する第2の手段を有することを特徴とする加入者装置。

【請求項15】加入者装置と通信を行う手段を有する端末装置において、

上記加入者装置は、パケット通信網に接続されており、パケット通信網上の閥門装置と通信を行う手段と、加入者毎の位置情報やサービス情報を備えるサービス制御装置と通信を行う手段を有し、

上記端末装置が上記パケット通信網上或いは他の通信网上的装置と情報の送受信を開始する前に、上記閥門装置に、予め定められた手順に従ってパケットの送受信を可能にするための制御信号を送信すると、

上記閥門装置は受信した制御信号から企業網内の装置との通信要求を検出し、

上記閥門装置が、上記加入者装置に、上記閥門装置自身の識別情報を含む制御信号を送信し、

上記端末装置が、上記制御信号を受信した上記加入者装置から上記閥門装置の識別情報を含む制御信号を受信した場合、

上記端末装置が、上記閥門装置の識別情報を利用して、送信パケットが、上記閥門装置を中継するようにパケットを組み立てる第3の手段を有することを特徴とする端末装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】IPv6移動体パケット通信網におけるパケット転送方法に関する。特にIPv6移動体パケット通信網とIPベース網の連携システムにおけるモバイルVPNサービス提供方法に関する。

【0002】

【従来の技術】インターネット及び移動通信サービスは、急速に普及している。

【0003】インターネットにおける通信は、事実上の標準であるIP(Internet Protocol、RFC791)プロトコルを用いるIPパケットの送信により行う。インターネットに接続される装置には、各装置を識別するため、世界で一意にIPアドレスが割り

当てられる。IPパケットのルーティングは、IPアドレスを使って行う。

【0004】IPパケットを受信した装置は、IPパケットのヘッダに含まれる着信先IPアドレスを調べる。装置自身に着信先IPアドレスを有する端末が存在しない場合、各装置は、ルーティングテーブルを利用して、IPパケットを隣接ノードに転送する。ルーティングテーブルとは、IPアドレスと隣接ノードの対応表である。

【0005】現在利用しているIPv4アドレスは、インターネットの普及に伴い枯渇する恐れがある。そこで、新しいアドレス体系であるIPv6アドレスの検討が行われている(Internet Protocol, Version 6 (IPv6) Specification, RFC 2460)。

【0006】IPv6は、拡張ヘッダの中で様々な機能を規定できる。IPv6拡張ヘッダは、IPv6ヘッダとペイロードの間に挿入される。経路制御ヘッダは、IPv6拡張ヘッダの1つである。経路制御ヘッダを利用すれば、パケット送信者は、パケットが通過すべき中間ノードを指定できる。

【0007】インターネットを利用するサービスとして、VPN(Virtual Private Network)が注目されている。VPNサービスには、LAN間接続VPNサービスとリモート・アクセスVPNサービスがある。LAN間接続VPNサービスは、LAN間接続にインターネットを利用するサービスである。リモート・アクセスVPNサービスは、外出中のユーザに企業内の装置へのアクセスを提供するサービスである。リモート・アクセスVPNサービスは、VPNへのアクセス機能を持つ装置と企業内のVPN装置との間の通信にインターネットを利用する。外出中のユーザは、ダイヤルアップ接続等でVPNアクセス機能を持つ装置に接続する。

【0008】VPNアクセス機能を備える装置とVPN装置の間の通信は、セキュリティを確保するため、トンネルを利用する。VPNアクセス機能を備える装置は、ユーザからIPパケットすると、受信パケットにVPN装置宛のヘッダを付加し(カプセル化)、VPN装置に送信する。VPN装置は、先に付加されたヘッダをとり(デカプセル化)、元のIPパケットを復元する。VPN装置は、元のIPパケットヘッダの宛先アドレスに書かれている装置宛にIPパケットを送信する。VPNに利用するトンネルをVPNトンネルと呼ぶ。VPNトンネルには、例えば、L2TP(Layer Two Tunneling Protocol, RFC 2661)がある。

【0009】近年の移動通信サービスでは、データ通信の割合が増加している。移動通信網において、データ通信を効率的に提供するため、移動体パケット通信網の検討が活発化している。移動体パケット通信網の例とし

て、PDC-P(PDC-Packet)やGPRS(General Packet Radio Service)がある。第3世代移動体通信システムIMT-2000においても高速パケット通信サービスの提供が予定されている。現在、移動体パケット通信網の上位通信プロトコルとして、IP(Internet Protocol)が普及している。

【0010】移動体パケット通信網において、IPプロトコルによる通信サービスを提供するため、通信事業者は移動端末にIPアドレスを割り当てる必要がある。移動端末の急増とIPv4アドレスの枯渇に伴い、移動端末にIPv6アドレスを割り振ることが予想される。

【0011】一般に移動体通信網は、無線アクセス網とコア網からなる。無線アクセス網は、基地局や基地局制御装置から構成される。コア網は、加入者ノードや閥門ノードから構成される。

【0012】移動体通信網における通信形態は、移動端末発固定端末着、固定端末発移動端末着、移動端末発移動端末着の3種類に分類される。

【0013】以下、例として、GPRS方式ベース移動端末発移動端末着のパケット通信手順を説明する。

【0014】GPRS方式ベース移動体パケット通信網の移動端末は、まず、端末自身の位置情報を移動体パケット通信網に登録する。次に、GPRS独自の信号手順を利用して、発信端末がパケットの送受信を行えるようにするため、発信端末と閥門ノードの間で制御信号を送信する。その後、移動端末は、着側移動端末に、IPパケットを送信する。

【0015】移動端末が着側移動端末宛に送信したIPパケットは、移動端末が在圏する加入者ノードを通過する。上記加入者ノードは、受信IPパケットに、発側の本拠地(ホーム)閥門ノード宛のヘッダを付加し(カプセル化)、発側ホーム閥門ノードにパケットを送信する。発側ホーム閥門ノードは、先に付加されたヘッダをとり(デカプセル化)、元のIPパケットを復元する。発側ホーム閥門ノードは、元のIPパケットヘッダの宛先アドレスに含まれる着側移動端末のIPアドレスから、着側移動端末のホーム閥門ノードを特定し、IPパケットを転送する。着側ホーム閥門ノードは、IPパケットヘッダの宛先アドレスから、着側移動端末が在圏する加入者ノードを特定する。着側ホーム閥門ノードは、再びIPパケットをカプセル化して、着側移動端末の在圏加入者ノードに向けてIPパケットを送信する。在圏加入者ノードは、受信パケットをデカプセル化して元のIPパケットを復元した後、着側移動端末にIPパケットを転送する。以上の処理により、発側移動端末が送信したIPパケットは、着側移動端末に到着する。

【0016】IPパケットをカプセル化した後、デカプセル化されて元のIPパケットを復元するまでの区間は、トンネルと呼ばれる。移動通信に利用するトンネル

をモバイルトンネルと呼ぶ。モバイルトンネルは、移動ユーザを追跡するために必要である。

【0017】一方、IETFは、IPv6アドレス対応のMobile IP仕様を検討中である。Mobile IP v6の発信端末は、プロバイダが着移動端末に割り当てたhome address宛にパケットを送信する。着移動端末のHome Agentは、上記home address宛パケットを受信する。上記Home Agentは、受信パケットに着移動端末の在圏アドレスを含むヘッダを付加し、着移動端末に転送する。在圏アドレスとは、移動端末の在圏網が移動端末に動的に割り当てるIPアドレスである。

【0018】パケットを受信した着移動端末は、発信端末に着移動端末自身の在圏アドレスを含む制御信号を送信する。上記発信端末は、上記制御信号に含まれる着移動端末の在圏アドレス情報を記憶する。上記発信端末が着移動端末の在圏アドレス情報を保持する場合、発信端末は着移動端末にパケットを送信する時、着移動端末の在圏アドレスを利用できる。

【0019】モバイルVPNサービスは、第3世代移動体通信システム(IMT-2000)の主要サービスになると予想されている。モバイルVPNサービスは、リモート・アクセスVPNの1形態であり、外出中のユーザが移動体パケット通信網を利用して、企業内の装置にアクセスするサービスである。モバイルVPNサービスは、移動端末発固定端末着の通信である。

【0020】モバイルVPNサービスを提供するため、特願2000-97813に記載されているように、移動体パケット通信網の関門ノードは、VPNアクセスサーバ機能を備える。モバイルVPNサービスでは、関門ノードとVPN装置間の通信に、VPNトンネルを利用する。このため、移動端末が送信するパケットは、通信開始時にアクセスしたVPNアクセスサーバ機能付き関門ノードを必ず経由する必要がある。

【0021】

【発明が解決しようとする課題】現在の移動体パケット通信網は、加入者ノードと関門ノード間の通信にモバイルトンネルを利用する。加入者ノードと関門ノードが、パケットのカプセル化・デカプセル化処理を行う。この時、パケットのカプセル化・デカプセル化に伴う加入者ノードと関門ノードの処理が増加し、移動体パケット通信網のスループットが低下するという課題がある。

【0022】しかし、モバイルトンネルを利用しない場合、移動端末が送信するIPパケットは、IPヘッダに基づいてルーティングされる。このため、上記パケットが、該当端末用のVPNトンネルが設定されている関門ノードを必ず経由するとは限らない。パケットが上記関門ノードを通過しない場合、ユーザが、モバイルVPNサービスを利用できないという課題がある。

【0023】

【課題を解決するための手段】上記課題を解決するため、本発明によるIPv6移動体パケット通信網におけるパケット通信制御方法では、IPv6経路制御ヘッダを利用してパケットを転送する。関門ノードは、移動体パケット通信網で利用されている制御信号を活用して、移動端末に経路制御ヘッダの作成に必要な情報を送信する。

【0024】移動端末は、まず、端末自身の位置情報を移動体パケット通信網に登録する。次に、発信端末は、データパケットの送受信を可能にするため、加入者ノードに制御メッセージ(Activate PDP Context Request)を送信する。上記制御メッセージを受信した加入者ノードは、APN(Access Point Name)から関門ノードを特定する。加入者ノードは、次のいずれかの手段により、APNを取得する。移動端末の接続先が固定されている場合、APNは移動用サービス制御装置(M-SCP)に格納されており、移動端末の位置登録時に、加入者ノードがM-SCPから読み出す。移動端末の接続先が可変である場合、移動端末ユーザが入力したAPNが、Activate PDP Context RequestのAPNパラメータに設定される。

【0025】加入者ノードは、特定した関門ノードに、移動端末がデータパケットの送受信をできるようにするため、制御メッセージ(Create PDP Context Request)を送信する。上記メッセージには、APNパラメータが必ず含まれる。上記メッセージを受信した関門ノードは、受信メッセージ中のAPNパラメータから接続先の外部ネットワークを特定する。

【0026】ここで、関門ノードは、APNからモバイルVPNサービスの要求を検出する第1の手段を備える。モバイルVPNサービスを利用する場合、関門ノードは、関門ノード自身のIPアドレスを含む応答メッセージ(Create PDP Context Response)を加入者ノードに送信する。

【0027】上記加入者ノードは、上記関門ノードのIPアドレスを含むCreate PDP Context Responseを受信した時、上記関門ノードのIPアドレスを含むActivate PDP Context Acceptメッセージを移動端末に送信する第2の手段を備える。

【0028】上記加入者ノードが関門ノードから上記関門ノードのIPアドレスを含まない応答メッセージを受信した時、加入者ノードは移動端末に上記関門ノードのIPアドレスは通知しない。

【0029】移動端末は、加入者ノードから関門ノードのIPアドレスを含む応答メッセージを受信すると、パケット送信時に必ずIPv6経路制御ヘッダを利用する第3の機能を備える。移動端末は、送信パケットが、必

ず、該当端末のVPNトンネルが設定されている上記閥門ノードを通過するように、IPv6ヘッダとIPv6経路制御ヘッダを組み立てる。IPv6経路制御ヘッダを利用すれば、パケット送信者は、パケットが通過するべき中間ノードとして、上記閥門ノードを指定できる。

【0030】移動端末が、上記加入者ノードから閥門ノードのIPアドレスを含まない応答メッセージを受信した場合、移動端末は、パケット送信時にIPv6経路制御ヘッダは利用しない。

【0031】即ち、移動端末は、送信パケットの中継経路を指定しない。この場合、移動端末が送信するパケットは、各ノードが保持するルーティングテーブル情報に基づき転送される。従って、移動端末が送信するパケットは、特定の閥門ノードを中継するとは限らない。移動端末がモバイルVPNサービスを利用しない場合は、移動端末が送信するパケットは特定閥門ノードを通過する必要はないため、問題はない。

【0032】IPv6経路制御ヘッダを含むIPパケットを受信した閥門ノードは、まず、IPv6経路制御ヘッダを処理する。次に、受信パケットにVPNトンネル用の付加ヘッダを追加し、VPN装置宛に送信する。

【0033】移動端末がIPv6経路制御ヘッダを使ってパケットを送信すれば、上記移動端末は送信パケットの中継ノードに、該当端末のVPNトンネルが設定されている特定閥門ノードを指定できる。従って、モバイルトンネルを利用することなく、移動端末ユーザにモバイルVPNサービスを提供できる。

【0034】本発明によれば、移動体パケット通信網が上記1から上記3の手段を備えることにより、モバイルトンネルを利用せずに、移動端末ユーザにモバイルVPNサービスを提供できる。

【0035】移動体パケット通信網において、IPv6機能を活用することにより、ネットワーク提供者は、通信サービスを効率的に提供できる。

【0036】

【発明の実施の形態】本発明の第1の実施の形態を図面を用いて説明する。

【0037】図1は、本発明によるモバイルVPNサービスをサポートするネットワークの構成例を示す。

【0038】モバイルVPNサービスをサポートするネットワークは、移動体パケット通信網12とインターネット15とLAN14から構成される。本発明では、移動体パケット通信網12とLAN14は、IPv6アドレスを利用する。

【0039】移動体パケット通信網12は、無線アクセス網5とコア網1から構成される。

【0040】移動体パケット通信網12のコア網1は、複数の加入者ノード4と、複数の閥門ノード3から構成される。加入者ノード4、及び、閥門ノード3は、共通線信号網11を介してM-SCP6に接続される。

【0041】閥門ノード3は、ISP13、或いは、Internet15など、移動体パケット通信網12以外の網とインターネットプロトコルによって通信する手段を持つ。また、閥門ノード3bは、VPNアクセスサーバ機能を備え、LAN14のVPN装置2にアクセスできる。

【0042】移動体パケット通信網12の無線アクセス網5は、複数の基地局(BTS)9(9a、9b)と、複数の基地局制御装置(RNC)10(10a、10b)によって構成される。

【0043】M-SCP6は、加入者情報と、端末の位置情報と、加入者に提供する付加サービスのプログラムを備える。

【0044】LAN14には、VPN装置2と、各種情報を提供するサーバ18が接続される。LAN14に、VPNサービス加入者の認証情報を備えるRADIUS(Remote Authentication Dial IN User Service)サーバ16やVPNサービスを利用する端末にIPアドレスを割り当てるDHCP(Dynamic Host Configuration Protocol)サーバ17を接続してもよい。

【0045】VPN装置2は、Internet15とインターネットプロトコルで通信する手段を持つ。

【0046】図2は、閥門ノード3の構成を示す。閥門ノード3は、加入者ノード4や他網との間の信号を制御するCPU31と、メモリ32と、共通線信号網との間の信号線35を終端する信号線終端部33と、他のIP網との間の信号線36や、コア網1内の他のノードとの間の信号線37を終端するIP網インタフェース部34(34a、34b)をバス38で接続する構成となっている。

【0047】CPU31と加入者ノードや他網との間の通信は、例えば、インターネットプロトコルを用いて行われる。

【0048】メモリ32は、他のIP網上の装置、或いは、コア網1上の装置と信号を送受信するプログラムや、移動端末がパケット通信に利用する制御情報を生成・修正・削除するプログラムや、LAN14のVPN装置2にアクセスするためのVPNアクセスサーバ機能を実現するプログラムや、図3に示すモバイルVPNサービスの検出を行うVPN判別処理ルーチン60や、図4に示すユーザ情報管理テーブル300を備える。

【0049】スイッチ39は、IP網インタフェース部34が接続され、ノード3内におけるスイッチング機能を実現する。

【0050】図4は、ユーザ情報管理テーブル300のテーブル構成を示す。本テーブルは、移動体パケット通信網加入者識別子(IMS I)301毎に生成された複数のエントリ(300-1~300-n)からなる。各

エントリは、IMS I30.1対応に、IPアドレス302と、端末が在圏する加入者ノードのIPアドレス303と、モバイルVPNサービスの利用を示すVPNフラグ304と、関門ノードとVPN装置間に設定したVPNトンネルを識別するVPNトンネル識別子305とVPNセッション識別子306を定義する。

【0051】図7は、端末(7、8)と関門ノード3との間で送信されるIPv6パケットのフォーマットを示す。IPパケット200は、IPv6ヘッダ210と、IPv6拡張ヘッダ220と、ペイロード230とからなる。IPv6では、IPv6ヘッダの次に拡張ヘッダ220を挿入できる。本発明では、拡張ヘッダの1つである経路制御ヘッダ(Routing Header)を利用する。従って、図7は、IPv6拡張ヘッダ220に、経路制御ヘッダを用いた場合のパケットフォーマットを示している。

【0052】IPv6ヘッダ210は、バージョン番号、トラフィッククラス、フローラベル、ペイロード長、後続ヘッダタイプ211、ホップ・リミット、送信元アドレス212、宛先アドレス213から構成される。後続ヘッダタイプ211は、IPv6ヘッダ210に後続するヘッダを識別する。ペイロード230に通常の上位プロトコル・データ単位(PDU)が入る場合には、後続ヘッダタイプ211に、上位プロトコルのプロトコル番号が設定される。IPv6拡張ヘッダ220がIPv6ヘッダに後続する場合は、後続ヘッダタイプ211にIPv6拡張ヘッダの種類を示す値が設定される。

【0053】宛先アドレス213には、通常、最終目的地のIPv6アドレスを設定する。ただし、経路制御ヘッダを用いる場合は、宛先アドレス213に、最終宛先ではなく、パケットを次に中継するべきノードのアドレスを設定する。

【0054】経路制御ヘッダは、後続ヘッダタイプ、ヘッダ長、ルーティング・タイプ、残余セグメント数221、アドレス222から構成される。残余セグメント数221には、未通過の中間ノード数を設定する。アドレス222には、パケットを中継するべき中間ノードのアドレスを設定する。アドレス222に、複数の中間ノードアドレスを設定してもよい。

【0055】本発明において、モバイルVPNサービスを利用する移動端末が送信するIPパケットは、IPv6ヘッダ210の後続ヘッダタイプ211に経路制御ヘッダタイプを、送信元アドレス212に端末のIPアドレスを、宛先アドレス213に関門ノードのIPアドレスをそれぞれ設定する。経路制御ヘッダのアドレス222には、移動端末が指定した通信先ノード18のIPアドレスを、残余セグメント数221には1をそれぞれ設定する。

【0056】図8は、関門ノード3とVPN装置2との間で、L2TPによるVPNトンネルを利用してパケッ

ト転送を行う場合のパケットフォーマット250を示す。

【0057】関門ノード3は、移動端末から受信したIPv6パケット200にVPNトンネル用のヘッダ240(IPヘッダ241、UDPヘッダ242、L2TPヘッダ243)を付加する。

【0058】関門ノード3がVPN装置2にパケットを送信する時、VPNヘッダ240に設定する情報は、次の通りである。IPヘッダ241の宛先アドレスにVPN装置2のIPアドレスを、送信元アドレスに関門ノード3のIPアドレスを設定する。UDPヘッダ242の宛先ポート番号に、データ送信先のアプリケーションが“L2TP”であることを示すポート番号「1701」を設定する。L2TPヘッダ243には、VPNトンネルを識別するIDや、VPNトンネル内のセッションを識別するIDを設定する。

【0059】図3は、モバイルVPNサービスの検出を行うVPN判別処理ルーチン60を示す。本ルーチンは、関門ノード3が、加入者ノード4から、Create PDP Context Requestメッセージを受信した場合に起動される。

【0060】VPN判別処理ルーチン60は、上記受信メッセージに必ず含まれるAPNを読み出し、モバイルVPNサービス要求の有無を判別する(ステップ61)。

【0061】モバイルVPNサービスが要求されている場合、関門ノード3は、VPNサービスへのアクセス可否を判断するため、例えば、LAN上のRADIUSサーバ16にVPN認証要求を送信する(ステップ62)。関門ノード3は、VPN認証処理待ち状態になる(ステップ63)。

【0062】VPN認証応答を受信した上記関門ノード3は、認証処理が正常終了したかを判別する(ステップ64)。正常終了時、上記関門ノード3は、自身のIPアドレスを含む応答メッセージ(Create PDP Context Response)を加入者ノード4に送信し(ステップ65)、本ルーチンを終了する。認証処理がエラー終了した時、上記関門ノード3は、エラー通知を含む応答を加入者ノード4に送信し(ステップ67)、本ルーチンを終了する。

【0063】ステップ61において、モバイルVPNサービス要求が検出されない場合、関門ノード3は、自身のIPアドレスを含まない応答を加入者ノード4に送信し(ステップ66)、本ルーチンを終了する。

【0064】上記加入者ノード4は、受信信号に関門ノード3のIPアドレスが含まれている時、移動端末に、上記関門ノード3のIPアドレスを含むActivate PDP Context Acceptメッセージを送信する。

【0065】上記加入者ノード4は、受信信号に関門ノ



ード 3 の IP アドレスが含まれない時、移動端末に、上記関門ノード 3 の IP アドレスを含まない `Activate PDP Context Accesspt` メッセージを送信する。

【0066】上記加入者ノード 4 は、受信信号にエラー通知が含まれる時、移動端末に、`Activate PDP Context Reject` メッセージを送信する。

【0067】次に、図 5 と図 6 に示す信号シーケンスに従って、図 1 に示したネットワークにおけるモバイル VPN サービスを提供するための処理手順を説明する。

【0068】図 5 は、移動体パケット通信網 12 に加入している移動端末 7 のユーザが、モバイル VPN サービスの利用を開始するために必要な処理手順を示す。

【0069】本発明の実施の形態では、移動体パケット通信網における制御信号に GPRS ベースの制御信号を用いて説明する。

【0070】移動端末 7 は、まず、移動端末の位置情報を移動体パケット通信網に登録する。

【0071】移動端末 7 は、移動体パケット通信網加入者識別子 (IMSI) を含む `Attach Request` メッセージ 100 を加入者ノード 4 a に送信する。加入者ノード 4 a は、受信メッセージ 100 に含まれる IMSI に基づいて、加入者情報を保持する M-SCP 6 を決定し、上記 M-SCP 6 に加入者情報読出要求メッセージ 101 を送信する。

【0072】上記 M-SCP 6 は、受信メッセージ 101 に含まれる IMSI に基づき、該当 IMSI の認証情報を読み出し、上記認証情報を含む加入者情報読出応答メッセージ 102 を上記加入者ノード 4 a に送信する。

【0073】上記加入者ノード 4 a は、移動端末 7 との間で認証処理を行う (103)。

【0074】認証処理が正常終了した場合、上記加入者ノード 4 a は、上記 M-SCP 6 に自身の IP アドレスを含む `Update Location` メッセージ 104 を送信する。

【0075】上記メッセージ 104 を受信した M-SCP 6 は、該当 IMSI の位置情報として、上記加入者ノード 4 a の IP アドレスを記憶する。続いて、上記 M-SCP 6 は、加入者ノード 4 a に加入者の契約情報等を含む `Insert Subscriber Data` メッセージ 105 を送信する。加入者ノード 4 a は、受信情報を記憶した後、M-SCP 6 に `Insert Subscriber Data Ack` メッセージ 106 を送信する。M-SCP 6 は、上記加入者ノード 4 a に、位置情報登録終了を示す `Update Location Ack` メッセージ 107 を送信する。上記メッセージ 107 を受信した加入者ノード 4 a は、`Attach Accept` メッセージ 108 を移動端末 7 に送信する。

【0076】移動端末 7 の接続先が固定的に登録されている場合、APN は、上記メッセージ 105 の契約情報に含まれる。

【0077】次に、移動端末 7 は、パケットの送受信を可能にするための処理を行う。移動端末 7 は、IMSI を含む `Activate PDP Context Request` メッセージ 109 を加入者ノード 4 a に送信する。

【0078】移動端末の接続先が可変である場合、移動端末ユーザが入力した APN が上記メッセージ 109 に含まれる。

【0079】上記加入者ノード 4 a は APN から関門ノードを特定し、関門ノード 3 b に APN を含む `Create PDP Context Request` メッセージ 110 を送信する。受信メッセージ 110 に含まれる APN は、通信要求に対応する通信網、又は、通信網上の装置を特定するために利用する。

【0080】上記関門ノード 3 b は、受信メッセージ 110 に含まれる加入者ノード IP アドレスをユーザ情報管理テーブル 300 の該当 IMSI に対応する加入者ノード IP アドレス 303 に格納する。次に、上記関門ノード 3 b は、図 3 に示す VPN 判別処理ルーチン 60 を起動し、モバイル VPN サービス要求の有無を判別する (111)。

【0081】モバイル VPN サービスが要求される場合、関門ノード 3 b は、図 4 に示すユーザ情報管理テーブル 300 の該当 IMSI に対応する VPN フラグ 304 を設定する。次に、VPN サービスへのアクセス可否を判断するため、関門ノード 3 b は、LAN 14 に接続される `RADIUS` サーバ 16 に認証要求 112 を送信する。認証に成功した場合、上記 `RADIUS` サーバ 16 は、上記関門ノード 3 b に、認証成功を示す認証応答 113 を送信する。

【0082】ここで、移動端末 7 に IP アドレスが割り振られていない場合、移動端末 7 に IP アドレスを割り振る手順を示す。IP アドレスを割り振る手段として、例えば、IPv6 対応 DHCP を利用する。

【0083】上記関門ノード 3 b は、LAN 14 に IP アドレス付与機能を持つ DHCP サーバを検出するための制御信号 (`DHCP Solicit`) 114 を送信する。上記信号 114 を受信した DHCP サーバ 17 は、自身のアドレス情報を含む応答信号 (`DHCP Advertise`) 115 を上記関門ノード 3 b に送信する。次に上記関門ノード 3 b は、上記 DHCP サーバ 17 に IP アドレス割り当て要求信号 (`DHCP Request`) 116 を送信する。上記信号 116 を受信した DHCP サーバ 17 は、移動端末 7 に IP アドレスを付与し (117)、上記関門ノード 3 b に上記 IP アドレスを含む応答信号 118 (`DHCP Replay`) を送信する。上記関門ノード 3 b は、割り当てられた I

Pアドレスを、図4に示すユーザ情報管理テーブル300の該当IMSIに対応するIPアドレス302に書きこむ。

【0084】次に閥門ノード3bは、閥門ノード3bとVPN装置2の間にVPNトンネルを設定する(119)。VPNトンネル設定後、加入者ノード3bは、該当ユーザのVPNトンネルIDとセッションIDを図4に示すユーザ情報管理テーブル300のVPNトンネルIDフィールド305とVPNセッションIDフィールド306に登録する。

【0085】閥門ノード3bは、割り当てられたIPアドレスと自身のIPアドレスを含むCreate PDP Context Responseを加入者ノード4aに送信する(120)。上記加入者ノード4aは、受信信号120に閥門ノード3bのIPアドレスが含まれる場合、移動端末7に、上記閥門ノード3bのIPアドレスと移動端末7に割り当てられたIPアドレスを含むActivate PDP Context Acceptを送信する(121)。

【0086】上記移動端末7は、受信信号121に含まれる閥門ノード3bのIPアドレスを記憶し、IPv6パケット通信に利用する。

【0087】ステップ111において、モバイルVPNサービスの要求が検出されない場合の処理を以下に示す。閥門ノード3bは、加入者ノード4aに閥門ノード3b自身のIPアドレスを含まないCreate PDP Context Response 120を送信する。上記加入者ノード4aは、移動端末7に上記閥門ノード3bのIPアドレスを含まないActivate PDP Context Accept 121を送信する。

【0088】図6は、図5に示した処理を完了した移動端末7が、パケットデータの送信する時の処理手順を示す。特に、移動端末7は加入者ノード4aから閥門ノード3bのIPアドレス情報を受信した場合を示す。

【0089】移動端末7は、図7に示したIPv6経路制御ヘッダを利用して、IPv6パケットを送信する。移動端末7は、以下に示すようにIPv6パケット131の設定を行い、パケットを送信する。IPv6ヘッダ210の宛先アドレス213に閥門ノード3bのIPアドレスを設定する。IPv6ヘッダ210の送信元アドレス212に移動端末7のIPアドレスを設定する。IPv6ヘッダ210の後続ヘッダ211に経路制御ヘッダが続くことを示す値“43”を設定する。IPv6経路制御ヘッダ220のアドレス情報222にLAN14内のサーバ18のIPアドレスを設定する。残余セグメント数221に1を設定する。

【0090】上記IPv6パケット131を受信した閥門ノード3bは、IPv6経路制御ヘッダを処理する。具体的には、IPv6ヘッダ210の宛先アドレス21

3にサーバ18のIPアドレスを設定し、IPv6経路制御ヘッダ220のアドレス情報222に閥門ノード3bのIPアドレスを設定し、残余セグメント数221を1から0に変更する。

【0091】上記閥門ノード3bは、サーバ18のIPアドレスのネットワークプレフィックスからモバイルVPNサービスを利用中であることを判断し、VPN装置2のIPアドレスを特定する。VPN装置2のIPアドレスは、VPNヘッダ240内のIPヘッダ241の宛先アドレスに設定される。

【0092】上記閥門ノード3bは、受信パケット131のIPv6ヘッダ210内の送信元アドレス212を検索キーとして、ユーザ情報管理テーブル300から該当移動端末7のVPNトンネルID305とVPNセッションID306を読み出す。上記VPNトンネルIDとVPNセッションIDは、VPNヘッダ240内のL2TPヘッダ243に設定される。

【0093】閥門ノード3bは、受信パケット131に、図8に示すVPNヘッダ240を付加し、VPN装置2宛にパケット132を送信する。

【0094】上記VPNヘッダ240付きパケット132を受信したVPN装置2は、VPNヘッダ240を取り外し、元のIPパケットに含まれる宛先IPアドレスが示すサーバ18に、IPパケット133を転送する。

【0095】以上の処理を行うことにより、移動端末7がサーバ18に送信するIPパケットは、必ず該当端末のVPNトンネルが設定されている閥門ノード3bを通過する。従って、IPv6移動体パケット通信網において、モバイルトンネルを利用することなく、モバイルVPNサービスを提供することが可能になる。

【0096】次に、移動端末7が、加入者ノード4aから閥門ノード3bのIPアドレス情報を受信しなかった場合の処理手順を示す。

【0097】移動端末7は、以下に示すようにIPv6パケット131の設定を行い、パケットを送信する。

【0098】IPv6ヘッダ210の宛先アドレス213にLAN14内のサーバ18のIPアドレスを設定する。IPv6ヘッダ210の後続ヘッダ211に上位プロトコルのプロトコル番号(例：上位プロトコルがTCPである場合には、“6”)を設定する。IPv6パケット131は、IPv6ヘッダ210とペイロード230とからなる。IPv6パケット131は、経路制御ヘッダ220を含まない。従って、移動端末7は、送信パケットの中継経路を指定しないため、送信パケットが閥門ノード3bを通過するとは限らない。移動端末がモバイルVPNサービスを利用しない場合、移動端末7が送信するパケットは、各ノードのルーティングテーブルに情報に基づき転送される。

【0099】

【発明の効果】以上の実施の形態の説明から明らかなよ

うに、本発明によれば、IPv6移動体パケット通信網において、IPv6の経路制御ヘッダを活用し、移動端末が送信するIPパケットが必ず特定の関門ノードを通過するように指定できる。従って、モバイルトンネルを利用することなく、モバイルVPNサービスを提供することが可能になる。IPv6の機能を活用して通信サービスを提供することにより、効率的な通信サービスの提供ができる。

【図面の簡単な説明】

【図 1】移動体パケット通信網の構成の一例を示す図。 10

【図2】 関門ノードの構成を示す図。

【図3】 閤門ノードで行うモバイルVPNサービス要求を判別するフローチャート。

【図4】 関門ノードが保持するユーザ情報管理テーブル

構成を示す図。

【図5】本発明における、端末の発信処理手順を示す信号シーケンス。

【図6】本発明における、通信処理手順を示す信号シーケンス。

【図 7】 移動端末から関門ノードに送信される I P v 6 パケットのフォーマット。

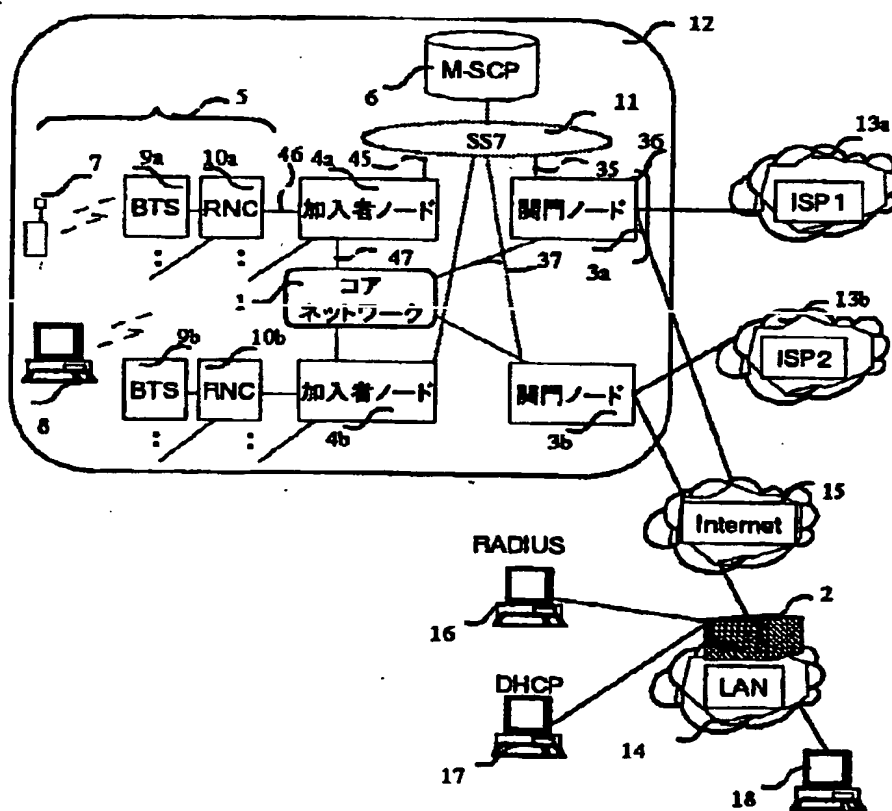
【図8】 閥門ノードからVPN装置に送信されるIPパケットのフォーマット。

【符号の説明】

2・・・VPN装置、3・・・閥門ノード、4・・・加入者ノード、6・・・移動サービス用サービス制御装置、7・・・移動端末、14・・・LAN、18・・・サーバ。

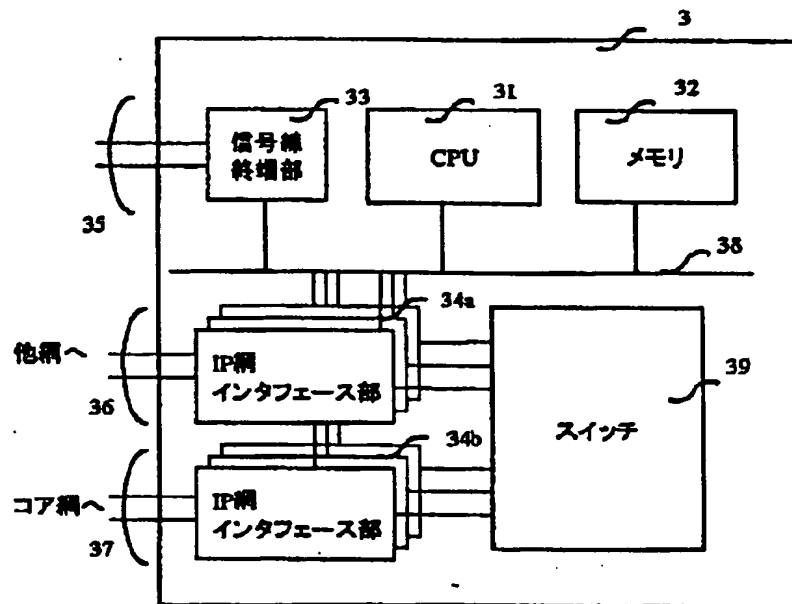
【图 1】

图 1



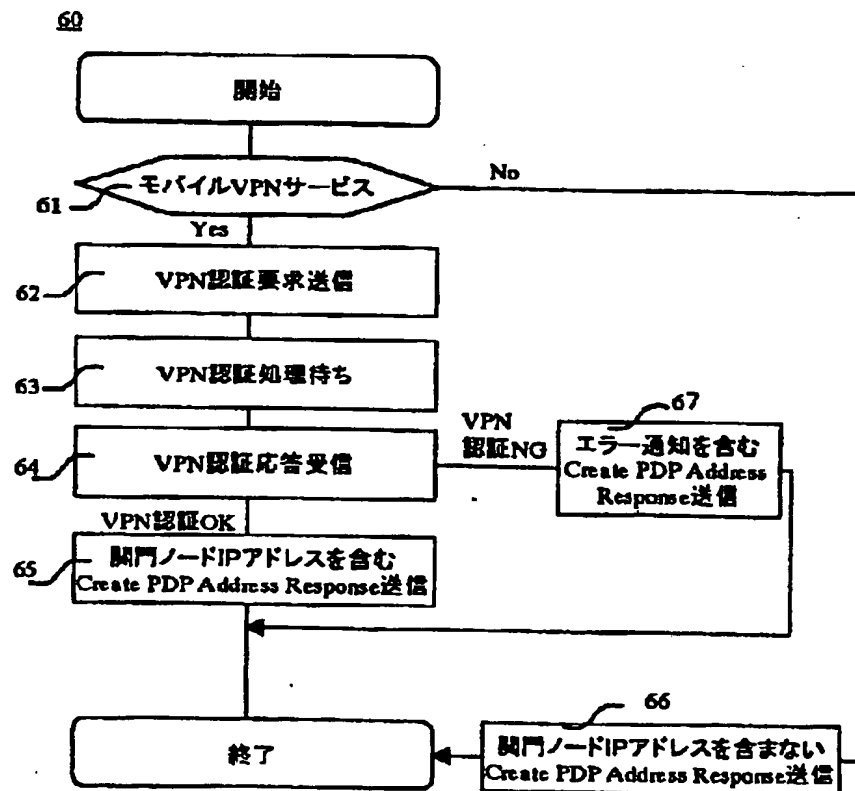
【図2】

図2



【図3】

図3



【図 4】

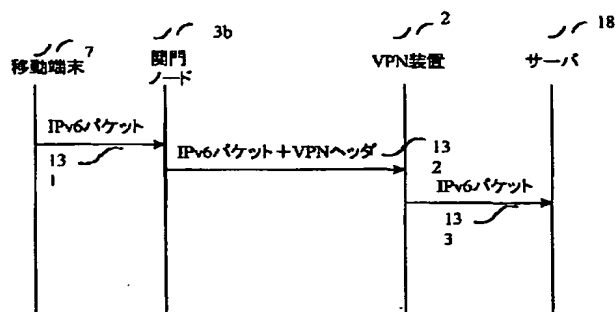
図 4

300 ユーザ情報管理テーブル

301 IMSI	302 IP address	303 加入者ノード IP address	304 VPN フラグ	305 VPN トンネルID	306 VPN セッションID
0123456789	133.144.12.34	133.150.1.2	1	any	300-1
0123987654	133.144.77.10	133.150.3.4	0	-	300-2
⋮	⋮	⋮	⋮	⋮	300-n

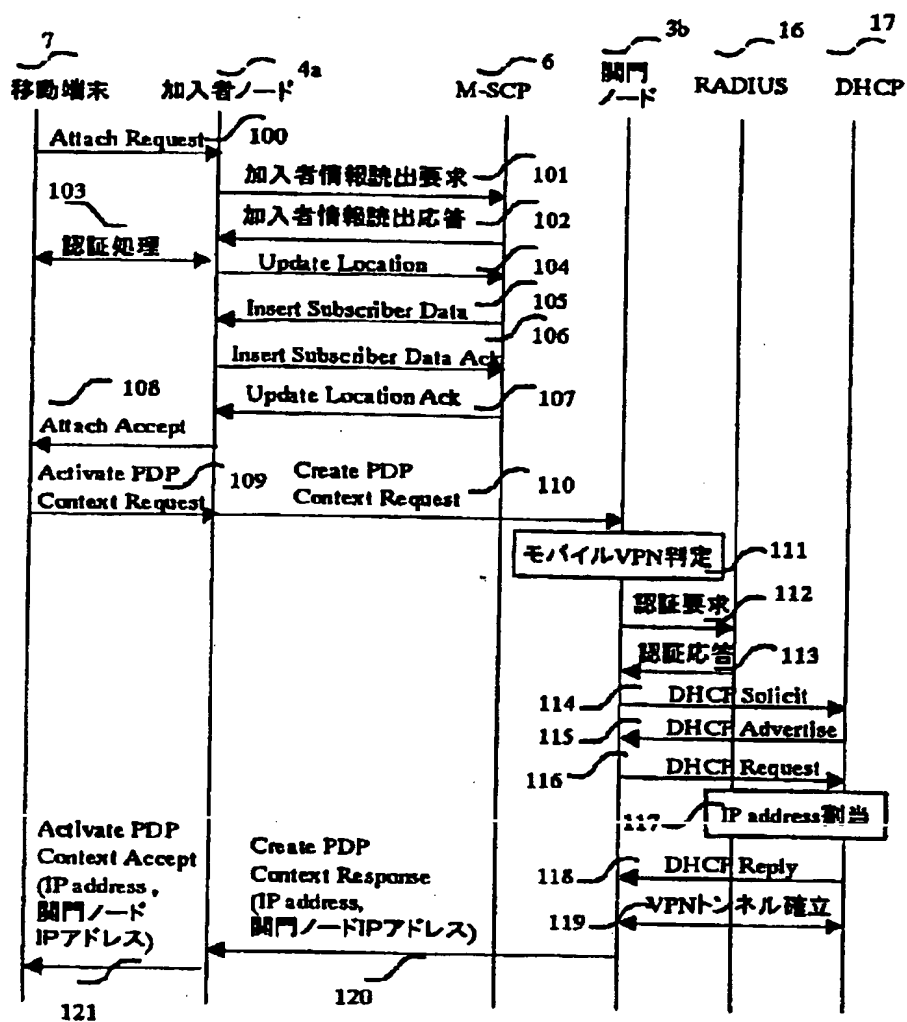
【図 6】

図 6



【図5】

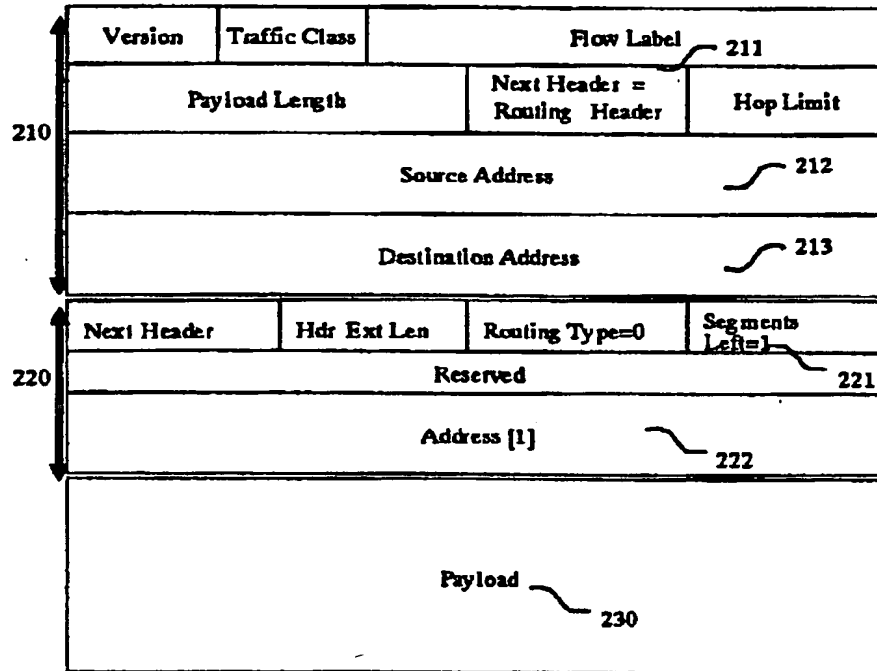
図5



【図 7】

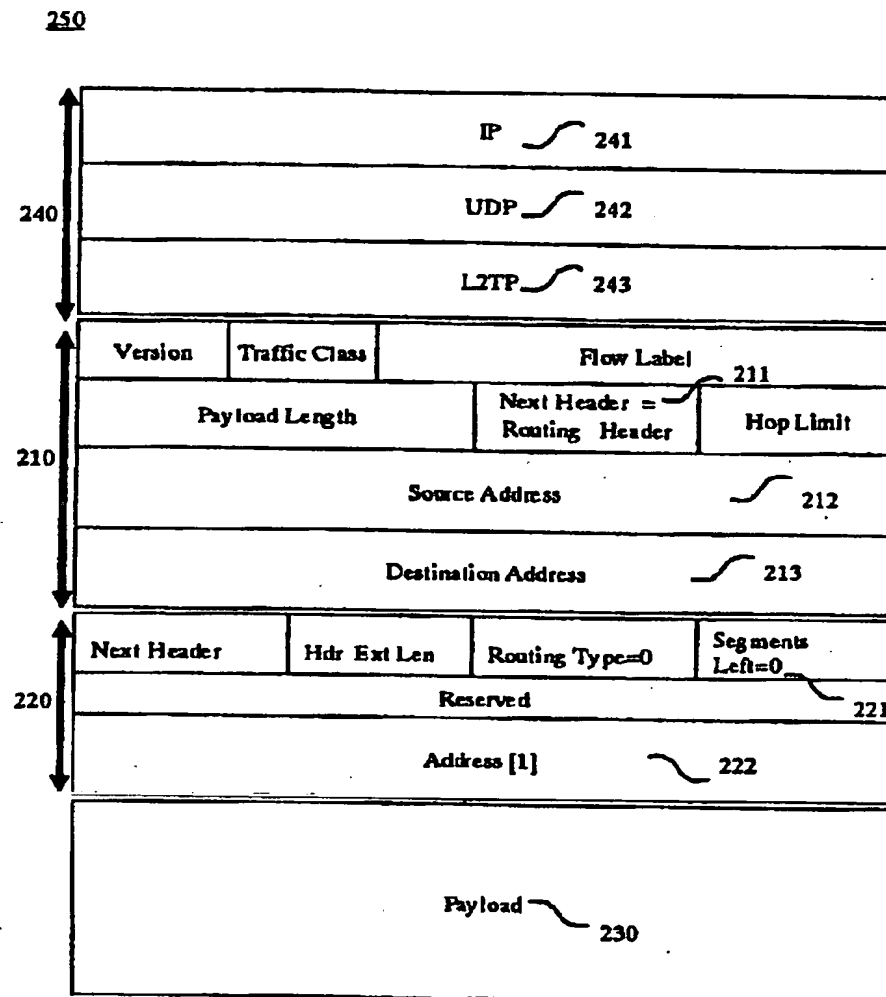
図 7

200



【図 8】

図 8



フロントページの続き

(72)発明者 大石 巧  
東京都国分寺市東恋ヶ窪一丁目280番地  
株式会社日立製作所中央研究所内

(72)発明者 柴田 治朗  
神奈川県横浜市戸塚区戸塚町216番地 株  
式会社日立製作所 I P システム事業部内

F ターム(参考) 5K030 GA19 HA08 HC01 HD03 HD05  
HD06 JL01 JT03 LA08 LB02  
LC06

5K033 AA09 CB14 CC01 DA01 DA19  
EA03

5K034 AA17 BB06 DD03 EE03 FF06  
HH01 HH02 LL01